	Application No.	Applicant(s)
Notice of Allowability	09/637,123	RAMANATHAN, RAMANATHAN
	Examiner	Art Unit	
	Arezoo Sherkat	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *3/18/2005*.

2. ☒ The allowed claim(s) is/are *35-45, 47, and 49-53*.

3. ☒ The drawings filed on *11 August 2000* are accepted by the Examiner.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All   b) ☐ Some*   c) ☐ None   of the:

        1. ☐ Certified copies of the priority documents have been received.

        2. ☐ Certified copies of the priority documents have been received in Application No. _____ .

        3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

    * Certified copies not received: _____ .

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.

    (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached

        1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.

    (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of
    Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)

2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)

3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____

4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material

5. ☐ Notice of Informal Patent Application (PTO-152)

6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *04/11/2005*.

7. ☒ Examiner's Amendment/Comment

8. ☐ Examiner's Statement of Reasons for Allowance

9. ☐ Other _____.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes

and/or additions be unacceptable to applicant, an amendment may be filed as provided

by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be

submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview

with Michael Barre on 4/11/2005.

The application has been amended as follows:

1-34. (canceled)

35. (currently amended) A method, comprising:

sending a network use digital contract from a policy administrator to a network

element, wherein the network use digital contract comprises a term to allow encrypted

communications from the network element to be decrypted by an entity other than

addressees of the encrypted communications;

sending a network monitoring digital contract from the policy administrator to

a network monitoring element;

wherein the network monitoring digital contract comprises a term to allow the

network monitoring element to monitor communications from the network element, even

if the encrypted communications are not addressed to the network monitoring element;

sending decrypting information from the policy administrator to the network

monitoring element in accordance with the network monitoring digital contract and

the network use digital contract, the decrypting information to allow the network

monitoring element to monitor a decrypted version of an encrypted communication

from the network element; and

before sending the network monitoring digital contract to the network

monitoring element, performing at least one operation from the group consisting of:

receiving a digital certificate for the network monitoring element at the policy

administrator; and

receiving a digital signature for the network monitoring element at the policy

administrator.

36. (previously presented) A method according to claim 35, where, before the

policy administrator sends the decrypting information to the network monitoring

element, the policy administrator performs operations comprising:

receiving, at the policy administrator, a request from the network monitoring

element for the decrypting information;

sending, from the policy administrator, a request to the network monitoring

element for the network monitoring digital contract;

receiving, at the policy administrator, the network monitoring digital contract from

the network monitoring element; and

authenticating the received network monitoring digital contract,

37. (previously presented) A method according to claim 35, wherein sending decrypting information to the network monitoring element comprises:

sending a decryption key from the policy administrator to the network monitoring element, the decryption key to allow the network monitoring element to decrypt the encrypted communication.

38. (previously presented) A method according to claim 35, wherein sending decrypting information to the network monitoring element comprises:

the policy administrator decrypting the encrypted communication; and

the policy administrator sending the decrypted communication to the network monitoring element.

39. (previously presented) A method according to claim 35, wherein, before the policy administrator sends the network monitoring digital contract to the network monitoring element, the policy administrator performs operations comprising:

receiving a digital certificate of the network monitoring element;

authenticating the digital certificate of the network monitoring element;

receiving a digital signature of the network monitoring element;

authenticating the digital signature of the network monitoring element;

writing contract terms in an electronic document;

writing the digital certificate of the network monitoring element and the digital

signature of the network monitoring element in the electronic document; and

writing a digital certificate of the policy administrator and a digital signature of the

policy administrator in the electronic document.

40. (previously presented) A method according to claim 39, wherein writing

contract terms in an electronic document comprises:

writing data in the electronic document to identify a time period during which the

network monitoring element will be allowed to monitor decrypted versions of encrypted

communications from the network element.

41. (previously presented) A method according to claim 35, wherein, before the

policy administrator sends the network use digital contract to the network element,

the policy administrator performs operations comprising:

receiving a digital certificate of the network element;

authenticating the digital certificate of the network element;

receiving a digital signature of the network element;

authenticating the digital signature of the network element;

writing contract terms in an electronic document;

writing the digital certificate of the network element and the digital signature

of the network element in the electronic document; and

writing a digital certificate of the policy administrator and a digital signature of

the policy administrator in the electronic document.

42. (previously presented) A method according to claim 35, wherein the term in the network use digital contract to allow encrypted communications from the network element to be decrypted by an entity other than addressees of the encrypted communications comprises:

data to indicate that the network element has agreed to allow encrypted communications from the network element to a second network element to be decrypted by an entity other than the second network element.

43. (currently amended) A method, comprising:

receiving, at a network monitoring element, a network monitoring digital contract from a policy administrator, wherein the network monitoring digital contract comprises a term to allow the network monitoring element to monitor encrypted communications from a network element managed by the policy administrator, even if the encrypted communications are not addressed to the network monitoring element;

sending, from the network monitoring element to the policy administrator, a request to monitor the encrypted communications;

sending the network monitoring digital contract from the network monitoring element to the policy administrator; and

after sending the network monitoring digital contract to the policy administrator, receiving, at the network monitoring element, decrypting information from the policy administrator, the decrypting information to allow the network monitoring element to

monitor decrypted versions of the encrypted communications from the network element; and

before receiving the network monitoring digital contract from the policy administrator, performing at least one Operation from the group consisting of:

sending a digital certificate for the network monitoring element to the policy administrator; and

sending a digital signature for the network monitoring element to the policy administrator.

44. (previously presented) A method according to claim 43, wherein the operation of receiving decrypting information from the policy administrator comprises:

receiving, from the policy administrator, a decryption key to allow the network monitoring element to decrypt the encrypted communications from the network element.

45. (previously presented) A method according to claim 43, wherein the operation of receiving decrypting information from the policy administrator comprises:

receiving, from the policy administrator, decrypted versions of the encrypted communications.

46. (canceled)

47. (currently amended) A method, comprising:

receiving, at a network element, a network use digital contract from a policy

administrator, wherein the network use digital contract comprises a term to indicate that

the network element has agreed to allow encrypted communications from the network

element to be decrypted by an entity other than addressees of the encrypted

communications;

sending an encrypted communication from the network element;

writing, into a log, information to allow the encrypted communication to be

decrypted, wherein the information is written into the log by the network element;

allowing the policy administrator to access the log to obtain the information to

allow the encrypted communication to be decrypted; and

before receiving the network use digital contract from the policy administrator,

performing at least one operation from the group consisting of:

sending a digital certificate for the network element to the policy administrator;

and

sending a digital signature for the network element to the policy administrator.

48. (canceled)

49. (currently amended) An article, comprising:

a machine accessible medium; and

instructions in the machine accessible medium, wherein the instructions,

when executed by a processing system, cause the processing system to provide

a policy administrator that performs operations comprising:

sending a network use digital contract to a network element, wherein the network

use digital contract comprises a term to allow encrypted communications from the

network element to be decrypted by an entity other than addressees of the encrypted

communications;

sending a network monitoring digital contract to a network monitoring element,

wherein the network monitoring digital contract comprises a term to allow the network

monitoring element to monitor communications from the network element, even if the

encrypted communications are not addressed to the network monitoring element;

sending decrypting information to the network monitoring element in accordance

with the network monitoring digital contract and the network use digital contract, the

decrypting information to allow the network monitoring element to monitor decrypted

versions of the encrypted communications from the network element; and

before sending the network monitoring digital contract to the network monitoring

element, performing at least one operation from the group consisting of:

receiving a digital certificate for the network monitoring element at the policy

administrator; and

receiving a digital signature for the network monitoring element at the policy

administrator.

50. (currently amended) An article, comprising:

a machine accessible medium; and

instructions in the machine accessible medium, wherein the instructions, when executed by a processing system, cause the processing system to provide a network monitoring element that performs operations comprising:

receiving a network monitoring digital contract from a policy administrator, wherein the network monitoring digital contract comprises a term to allow the network monitoring element to monitor communications from a network element managed by the policy administrator, even if the encrypted communications are not addressed to the network monitoring element;

sending, to the policy administrator, a request to monitor communications from the network element;

sending the network monitoring digital contract to the policy administrator; and

after sending the network monitoring digital contract to the policy administrator, receiving decrypting information from the policy administrator, the decrypting information to allow the network monitoring element to monitor decrypted versions of encrypted communications from the network element; and

before receiving the network monitoring digital contract from the policy administrator, performing at least one operation from the group consisting of:

sending a digital certificate for the network monitoring element to the policy administrator; and

sending a digital signature for the network monitoring element to the policy administrator.

51. (currently amended) An article, comprising:

a machine accessible medium; and

instructions in the machine accessible medium, wherein the instructions, when executed by a processing system, cause the processing system to provide a network element that performs operations comprising: receiving a network use digital contract from a policy administrator, wherein the network use digital contract comprises a term to indicate that the network element has agreed to allow encrypted communications from the network element to be decrypted by an entity other than addressees of the encrypted communications;

sending an encrypted communication from the network element;

writing, into a log, information to allow the encrypted communication to be decrypted, wherein the information is written into the log by the network element; and

allowing the policy administrator to access the log to obtain the information to allow the encrypted communication to be decrypted; and

before receiving the network us" digital contract from the policy administrator, performing at least one operation from the group consisting of:

sending a digital certificate for the network element to the policy administrator; and

sending a digital signature for the network element to the Policy administrator.

52. (currently amended) An apparatus comprising:

a processor;

a machine accessible medium in communication with the processor; and

instructions in the machine accessible medium, wherein the instructions, when

executed by the processor, enable the apparatus to operate as a policy administrator

that performs operations comprising:

sending a network use digital contract to a network element, wherein the

network use digital contract comprises a term to allow encrypted communications

from the network element to be decrypted by an entity other than addressees of the

encrypted communications; and

sending a network monitoring digital contract to a network monitoring element,

wherein the network monitoring digital contract comprises a term to allow the network

monitoring element to monitor communications from the network element, even if the

encrypted communications are not addressed to the network monitoring element;

sending decrypting information to the network monitoring element in accordance

with the network monitoring digital contract and the network use digital contract, the

decrypting information to allow the network monitoring element to monitor a decrypted

version of an encrypted communication from the network element; and

before sending the network monitoring digital contract to the network monitoring

element, performing at least one operation from the group consisting of:

receiving a digital certificate for the network monitoring element at the policy

administrator; and

receiving a digital signature for the network monitoring element at the policy

administrator.

53. (currently amended) An apparatus comprising:

a processor;

a machine accessible medium in communication with the processor; and

instructions in the machine accessible medium, wherein the instructions, when

executed by the processor, enable the apparatus to operate as a network element that

performs operations comprising:

receiving a network use digital contract from a policy administrator, wherein the

network use digital contract comprises a term to indicate that the network element has

agreed to allow encrypted communications from the network element to be decrypted

by an entity other than addressees of the encrypted communications;

sending an encrypted communication from the network element;

writing, into a log, information to allow the encrypted communication to be

decrypted, wherein the information is written into the log by the network element;

allowing the policy administrator to access the log to obtain the information to

allow the encrypted communication to be decrypted; and

before receiving the network use digital contract from the policy administrator,

performing at least one operation from the group consisting of:

sending a digital certificate for the network element to the policy administrator;

and

sending a digital signature for the network element to the policy administrator.

Allowable Subject Matter

Claims 35-45, 47, and 49-53 are allowed.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Arezoo Sherkat whose telephone number is (571) 272-3796. The examiner can normally be reached on 8:00-4:30 Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Arezoo Sherkat
Patent Examiner
Group 2131
April 12, 2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100